

LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
PERTEMUAN 6
(Snort dan Firewall Rule)



DISUSUN OLEH
Indah Sekar Ningrum (21/478139/SV/19241)

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
YOGYAKARTA

2023

I. Link Github

<https://github.com/indah0503/Praktikum-Keamanan-Informasi-Kelas-A/tree/Pertemuan-6>

II. Langkah – Langkah

A. Mempersiapkan Lingkungan Virtual

1. Luncurkan Oracle VirtualBox dan ubah CyberOps Workstation untuk mode Bridged, jika perlu. Pilih Mesin > Pengaturan > Jaringan.
2. Luncurkan VM CyberOps Workstation, buka terminal dan konfigurasi jaringannya dengan menjalankan skrip `configure_as_dhcp.sh`.

```
[analyst@secOps ~]$ sudo ./lab.support.files/scripts/configure_as_dhcp.sh
[sudo] password for analyst:
Configuring the NIC to request IP info via DHCP...
Requesting IP information...
IP Configuration successful.
```

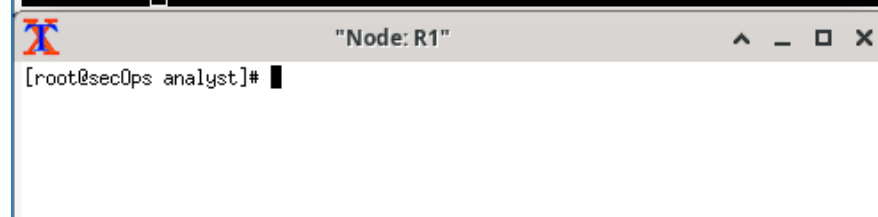
B. Firewall and IDS Logs

1. Dari VM CyberOps Workstation, jalankan skrip untuk memulai mininet.mininet.

```
[analyst@secOps ~]$ sudo ./lab.support.files/scripts/cyberops_extended_topo_no_fw.py
[sudo] password for analyst:
*** Adding controller
*** Add switches
*** Add hosts
*** Add links
*** Starting network
*** Configuring hosts
R1 R4 H1 H2 H3 H4 H5 H6 H7 H8 H9 H10 H11
*** Starting controllers
*** Starting switches
*** Add routes
*** Post configure switches and hosts
*** Starting CLI:
mininet> 
```

2. Dari prompt mininet, buka shell di R1 menggunakan perintah di bawah ini:

```
mininet> xterm R1
mininet> 
```



3. Dari shell R1, jalankan IDS berbasis Linux, Snort.

```
[root@secOps analyst]# ./lab.support.files/scripts/start_snort.sh
```

```

"Node: R1"
=====
+
=====
Run time for packet processing was 204.52485 seconds
Snort processed 1 packets.
Snort ran for 0 days 0 hours 3 minutes 24 seconds
  Pkts/min:      0
  Pkts/sec:      0
=====
Memory usage summary:
  Total non-mapped bytes (arena):      48541696
  Bytes in mapped regions (hblkhd):    22142976
  Total allocated space (uordblks):    38154560
  Total free space (fordblks):         10387136
  Topmost releasable block (keepcost): 101920
=====
Packet I/O Totals:
  Received:      1

```

4. Dari prompt mininet CyberOps Workstation VM, buka shell untuk host H5 dan H10.

```

mininet> xterm H5
mininet> xterm H10

```

5. H10 akan mensimulasikan server di Internet yang menghosting malware. Pada H10, jalankan skrip mal_server_start.sh untuk memulai server.

```

"Node: H10"
[root@secOps analyst]# ./lab.support.files/scripts/mal_server_start.sh
[root@secOps analyst]#

```

6. Pada H10, gunakan netstat dengan opsi -tunpa untuk memverifikasi bahwa server web sedang berjalan. Saat digunakan seperti yang ditunjukkan di bawah ini, netstat mencantumkan semua port yang saat ini ditetapkan ke layanan:

```

[root@secOps analyst]# netstat -tunpa
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80               0.0.0.0:*               LISTEN      3025/nginx: master

```

7. Di tab terminal R1 baru, jalankan perintah tail dengan opsi -f untuk memantau file /var/log/snort/alert secara real-time. File ini adalah tempat snort dikonfigurasi untuk merekam peringatan.

```

[root@secOps analyst]# tail -f /var/log/snort/alert

```

8. Dari H5, gunakan perintah wget untuk mengunduh file bernama W32.Nimda.Amm.exe.

```
"Node: H5"
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-02-20 23:50:33-- http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... connected.
HTTP request sent, awaiting response... 200 OK
Length: 345088 (337K) [application/octet-stream]
Saving to: 'W32.Nimda.Amm.exe.1'

W32.Nimda.Amm.exe.1 100%[=====>] 337.00K --.-KB/s in 0.003s

2023-02-20 23:50:33 (120 MB/s) - 'W32.Nimda.Amm.exe.1' saved [345088/345088]
```

9. Saat file berbahaya sedang transit R1, IDS, Snort, dapat memeriksa muatannya. Payload cocok dengan setidaknya satu tanda tangan yang dikonfigurasi di Snort dan memicu peringatan di jendela terminal R1 kedua (tab tempat tail -f berjalan). Entri peringatan ditunjukkan di bawah ini.

```
[root@secOps analyst]# tail -f /var/log/snort/alert
02/20-23:57:48.310046 [**] [1:1000003:0] Malicious Server Hit! [**] [Priority:
0] {TCP} 209.165.200.235:35364 -> 209.165.202.133:6666
```

Pada H5, gunakan perintah tcpdump untuk merekam peristiwa dan mengunduh file malware lagi sehingga Anda dapat merekam transaksi. Keluarkan perintah berikut di bawah ini mulai pengambilan paket:

```
[root@secOps analyst]# tcpdump -i H5-eth0 -w nimda.download.pcap &
[1] 3087
[root@secOps analyst]# tcpdump: listening on H5-eth0, link-type EN10MB (Ethernet
), capture size 262144 bytes
```

10. Pada H5, jalankan kembali perintah atau gunakan panah atas untuk memanggilnya kembali dari fasilitas riwayat perintah.

```
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-02-20 23:57:48-- http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... connected.
HTTP request sent, awaiting response... 200 OK
Length: 345088 (337K) [application/octet-stream]
Saving to: 'W32.Nimda.Amm.exe.2'

W32.Nimda.Amm.exe.2 100%[=====>] 337.00K --.-KB/s in 0.01s

2023-02-20 23:57:48 (24.6 MB/s) - 'W32.Nimda.Amm.exe.2' saved [345088/345088]
```

11. Hentikan pengambilan dengan membawa tcpdump ke latar depan dengan perintah fg.

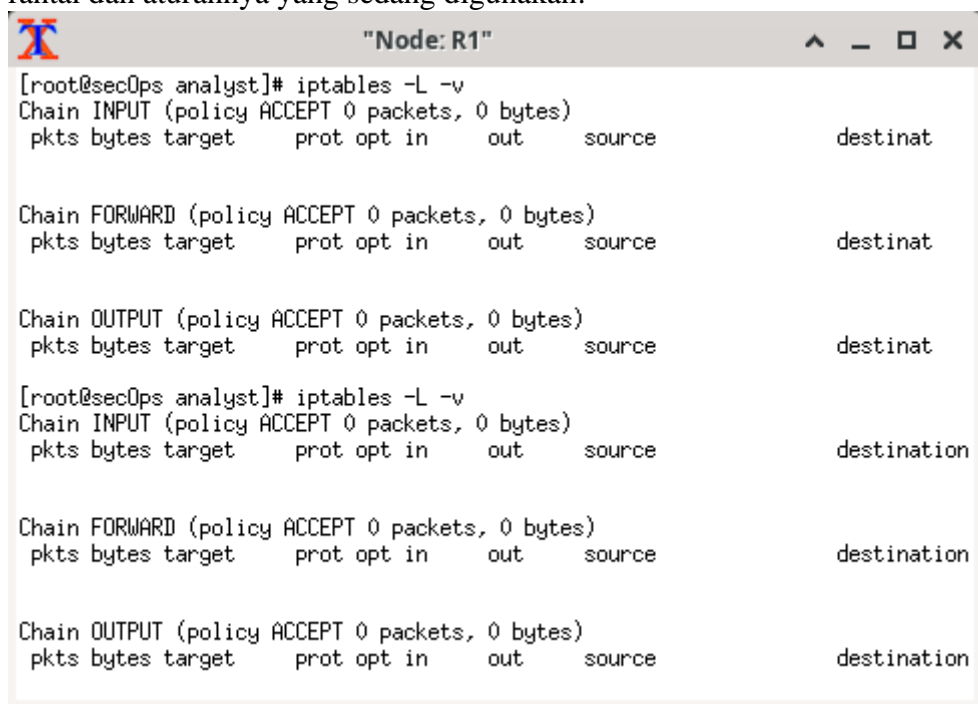
```
[root@secOps analyst]# fg
tcpdump -i H5-eth0 -w nimda.download.pcap
^C53 packets captured
53 packets received by filter
0 packets dropped by kernel
[root@secOps analyst]# █
```

12. Pada H5, Gunakan perintah ls untuk memverifikasi file pcap sebenarnya disimpan ke disk dan memiliki ukuran lebih besar dari nol:

```
[root@secOps analyst]# ls -l
total 1404
drwxr-xr-x 2 analyst analyst 4096 May 20 2020 Desktop
drwxr-xr-x 3 analyst analyst 4096 Apr 2 2020 Downloads
-rw-r--r-- 1 root root 16557 Feb 20 21:51 httpdump.pcap
-rw-r--r-- 1 root root 24 Feb 20 21:45 httpsdump.pcap
drwxr-xr-x 9 analyst analyst 4096 Jul 15 2020 lab.support.files
-rw-r--r-- 1 root root 349804 Feb 21 00:00 nimda.download.pcap
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 analyst analyst 345088 Feb 20 23:14 W32.Nimda.Amm.exe
-rw-r--r-- 1 root root 345088 Mar 23 2018 W32.Nimda.Amm.exe.1
-rw-r--r-- 1 root root 345088 Mar 23 2018 W32.Nimda.Amm.exe.2
```

C. Menyetel Aturan Firewall Berdasarkan IDS Alerts

1. Di VM CyberOps Workstation, mulai jendela terminal R1 ketiga.
2. Di jendela terminal R1 baru, gunakan perintah iptables untuk membuat daftar rantai dan aturannya yang sedang digunakan.



```

Node: R1
[root@secOps analyst]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

[root@secOps analyst]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

```

3. Agar komputer pengguna tidak terhubung ke server yang diidentifikasi di Langkah 1, tambahkan aturan berikut ke rantai FORWARD di R1:

```
[root@secOps analyst]# iptables -I FORWARD -p tcp -d 209.165.202.133 --dport 6666 -j DROP
[root@secOps analyst]#
```

4. Gunakan perintah iptables lagi untuk memastikan aturan telah ditambahkan ke rantai FORWARD. (Karena pada poin 3 melakukannya 2 kali)

```

[root@secOps analyst]# iptables -L -v
Chain INPUT (policy ACCEPT 6 packets, 612 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
 0      0 DROP      tcp  --  any    any    anywhere                209.165.202.133      tcp dpt:6666
 0      0 DROP      tcp  --  any    any    anywhere                209.165.202.133      tcp dpt:6666

Chain OUTPUT (policy ACCEPT 8 packets, 592 bytes)
 pkts bytes target    prot opt in     out     source                   destination

[root@secOps analyst]#
```

5. Pada H5, coba unduh file lagi:

```
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-02-21 00:10:21-- http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... failed: Connection timed out.
Retrying.

--2023-02-21 00:12:32-- (try: 2) http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666...
```

D. Hentikan dan Hapus Proses Mininet

1. Arahkan ke terminal yang digunakan untuk memulai Mininet. Hentikan Mininet dengan memasukkan exit di jendela terminal VM CyberOps utama.

```
mininet> exit
*** Stopping 0 controllers

*** Stopping 5 terms
*** Stopping 15 links
.....
*** Stopping 3 switches
S5 S9 S10
*** Stopping 13 hosts
R1 R4 H1 H2 H3 H4 H5 H6 H7 H8 H9 H10 H11
*** Done
[analyst@secOps ~]$
```

2. Setelah keluar dari Mininet, bersihkan proses yang dimulai oleh Mininet. Masukkan kata sandi cyberops saat diminta.

```
[analyst@secOps ~]$ sudo mn -c
[sudo] password for analyst:
*** Removing excess controllers/ofprotocols/ofdatapaths/pings/noxes
killall controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller u
dpbwtest mnexec ivs 2> /dev/null
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controlle
r udpbwtest mnexec ivs 2> /dev/null
pkill -9 -f "sudo mnexec"
*** Removing junk from /tmp
rm -f /tmp/vconn* /tmp/vlogs* /tmp/*.out /tmp/*.log
*** Removing old X11 tunnels
*** Removing excess kernel datapaths
ps ax | egrep -o 'dp[0-9]+' | sed 's/dp/nl:/'
*** Removing OVS datapaths
ovs-vsctl --timeout=1 list-br
ovs-vsctl --timeout=1 list-br
*** Removing all links of the pattern foo-ethX
ip link show | egrep -o '([_[:alnum:]]+-eth[[:digit:]]+)'
ip link show
*** Killing stale mininet node processes
pkill -9 -f mininet:
*** Shutting down stale tunnels
pkill -9 -f Tunnel=Ethernet
pkill -9 -f .ssh/mn
rm -f ~/.ssh/mn/*
*** Cleanup complete.
[analyst@secOps ~]$
```